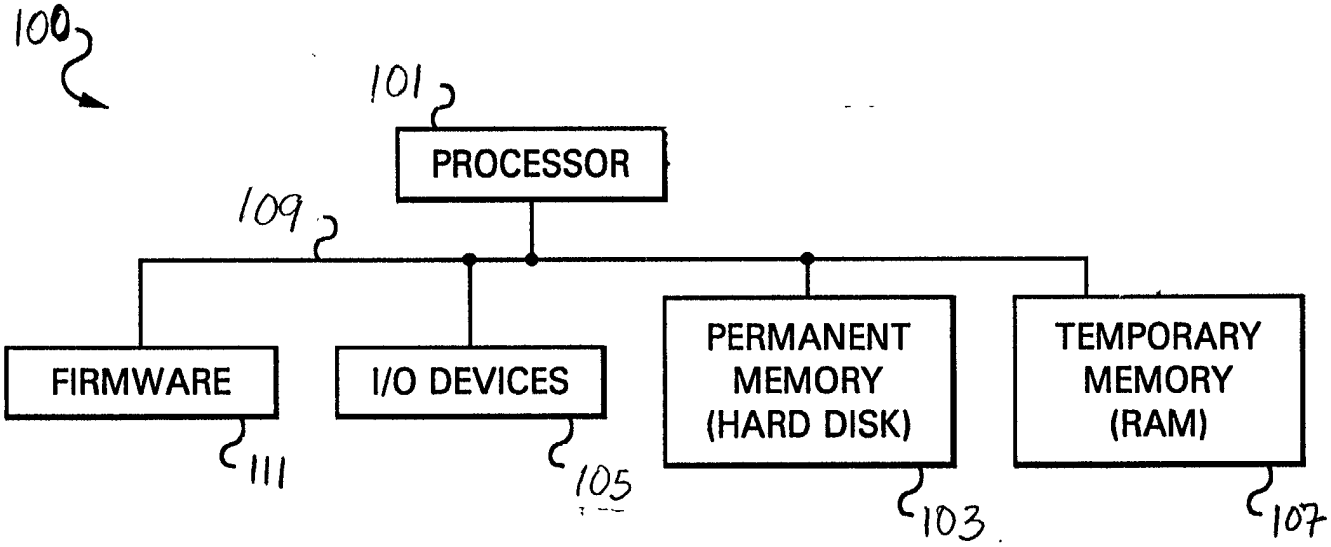
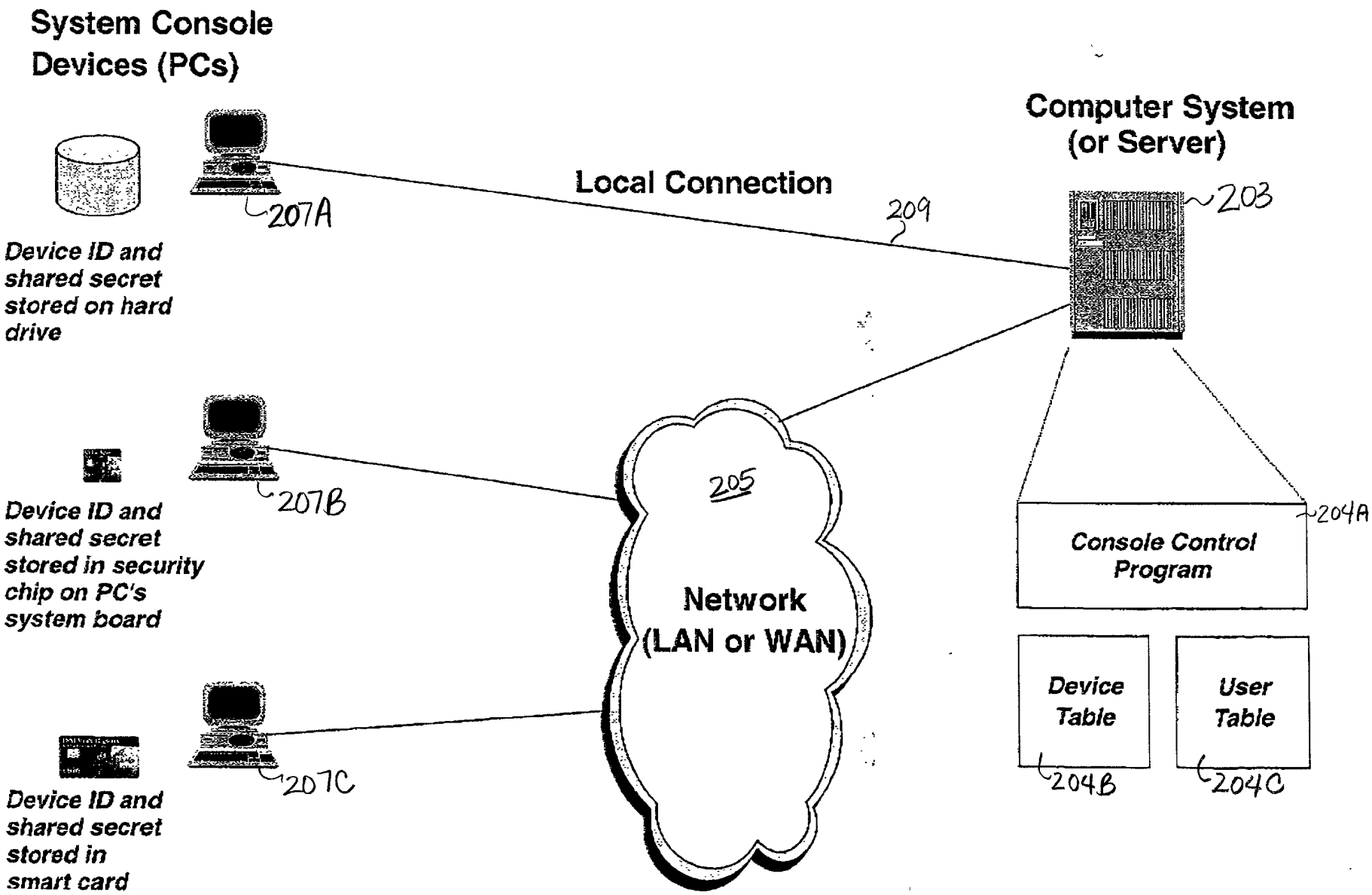


Fig. 1

FIG 2


System Console Devices (PCs)
Computer System (or Server)
Local Connection
209
207A
203
Device ID and shared secret stored on hard drive
207B
205
Device ID and shared secret stored in security chip on PC's system board
Network (LAN or WAN)
204A
Console Control Program
Device Table
User Table
204B
204C
207C
Device ID and shared secret stored in smart card

301

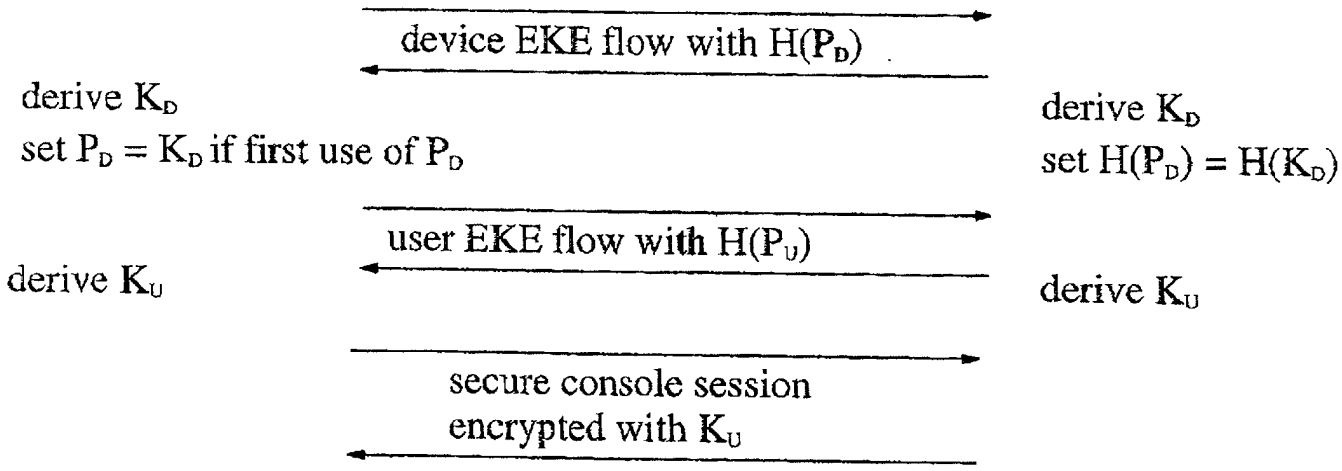
Op Console PC **OS/400**

Console session flow

Normal flow -
prompt for I_D, P_A, I_{Ux}, P_{Ux}

Setup wizard -
1)prompt for I_D, P_D, P_A, I_{Ux}, P_{Ux}
2)use PKCS-5 to encrypt P_D with P_A

Shipped with:
I_D = QCONSOLE, $H(P_D)$ = H(QCONSOLE
I_{U3} = QSECOFR, $H(P_{U3})$ = H(QSECOFR)
I_{U2} = 22222222, $H(P_{U2})$ = H(22222222)
I_{U1} = 11111111, $H(P_{U1})$ = H(11111111)



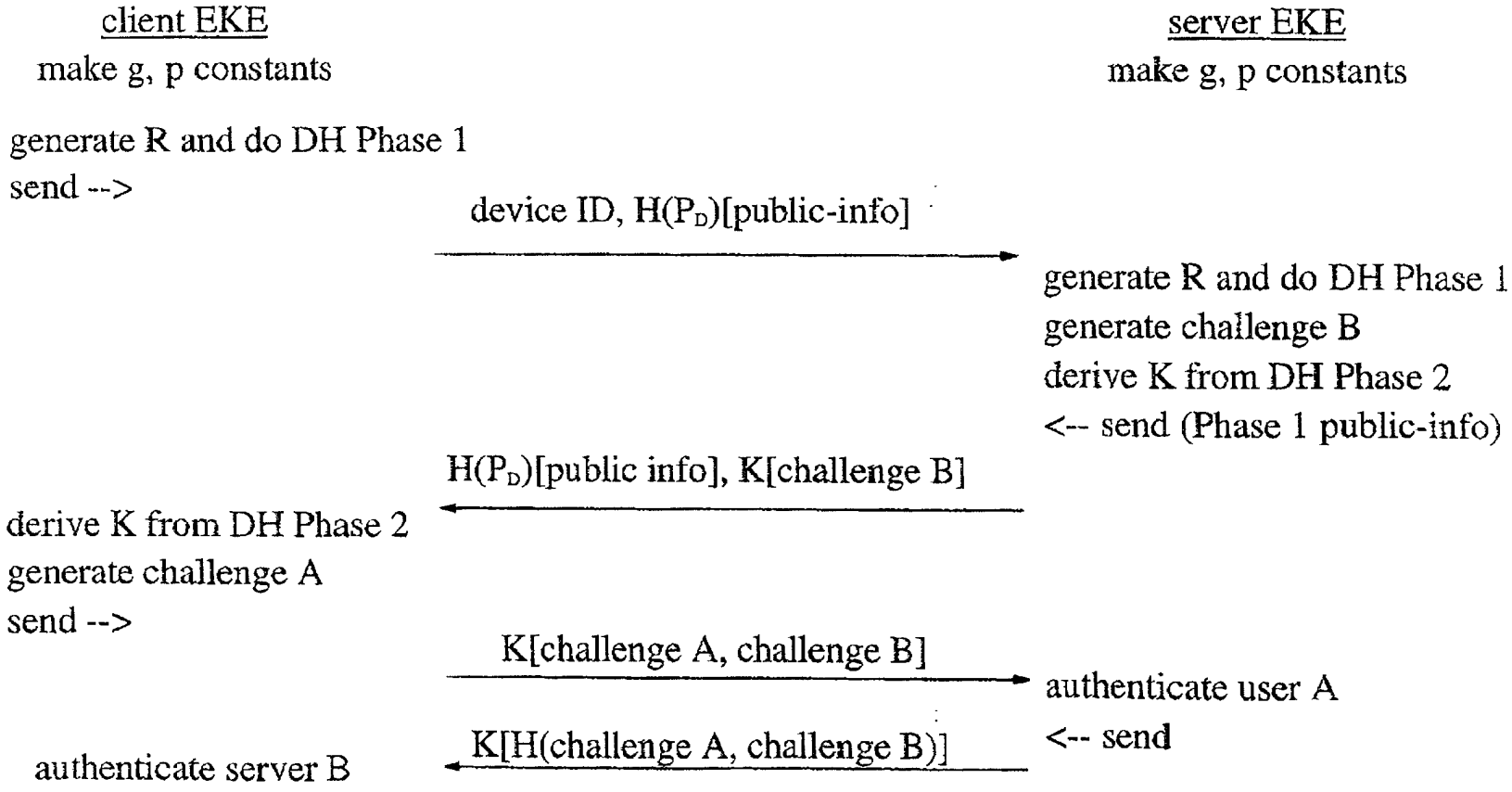
Legend:
I_D = Device identifier
P_D = Device shared secret
P_A = Access passphrase
I_{Ux} = User ID
P_{Ux} = User passphrase
K_D = Device session key
K_U = User session key

K = Random number
H(x) = Hash of x

NOTE: The first console session uses the well known shipped device identifier and user ID to access the iSeries. The device passphrase is modified in the initial flow ($P_D = K_D$). Therefore, the genesis device essentially "gets in free."

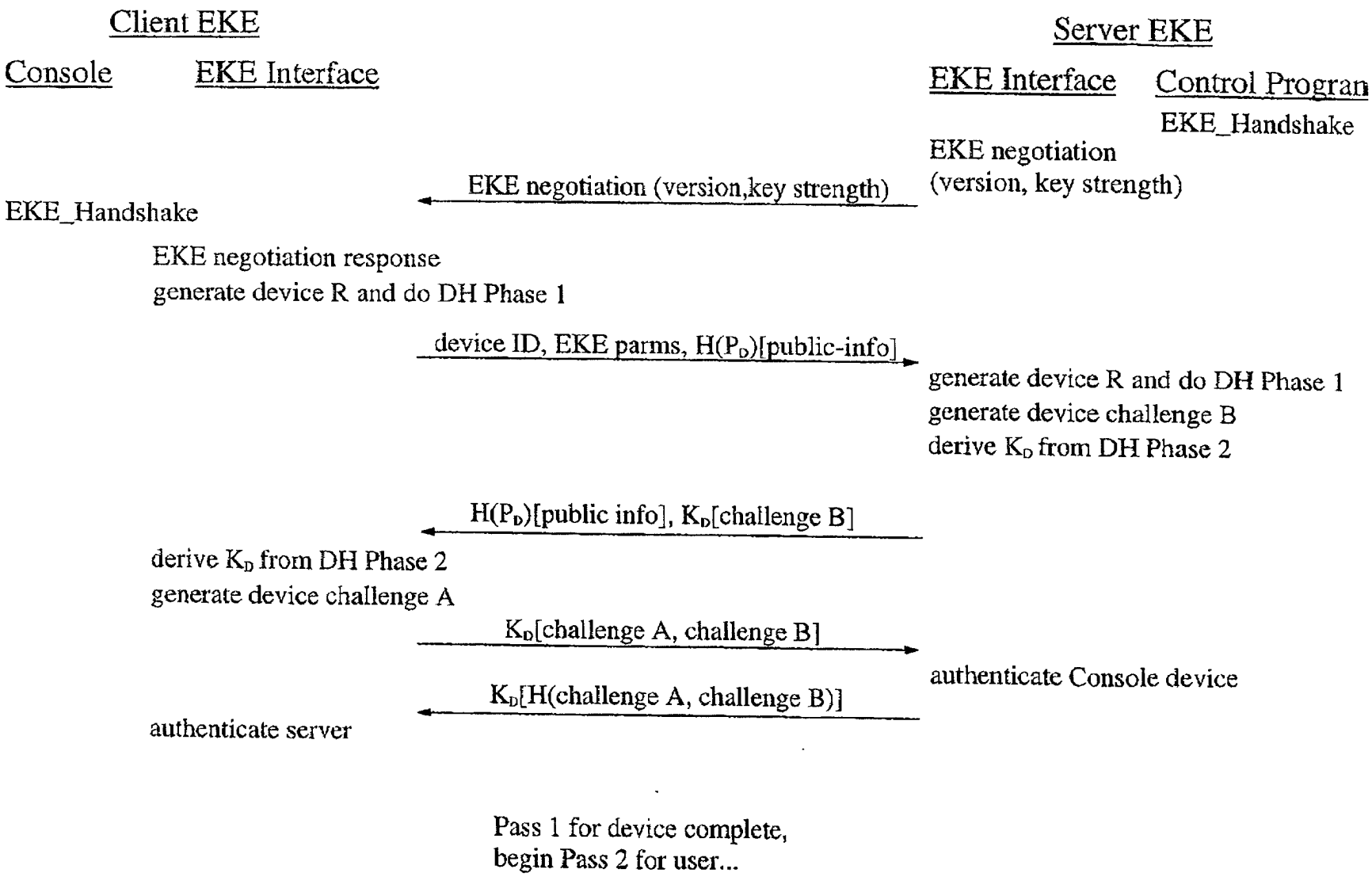
303

- generate DH parameters g and p
- where g = base; p = prime; these values do not have to be secret (public-info)
- make g and p constants in server and client EKE code



Refer to BSAFE Reference Manual for description of DH Phase 1& 2.

NOTE: The challenge strings must be a different length than the encryption block.


Client EKE
Console
EKE Interface
Server EKE
EKE Interface
Control Progran
EKE_Handshake
EKE negotiation
(version, key strength)
EKE negotiation (version,key strength)
EKE_Handshake
EKE negotiation response
generate device R and do DH Phase 1
device ID, EKE parms, H(P_D)[public-info]
generate device R and do DH Phase 1
generate device challenge B
derive K_D from DH Phase 2
H(P_D)[public info], K_D[challenge B]
derive K_D from DH Phase 2
generate device challenge A
K_D[challenge A, challenge B]
authenticate Console device
K_D[H(challenge A, challenge B)]
authenticate server
Pass 1 for device complete,
begin Pass 2 for user...

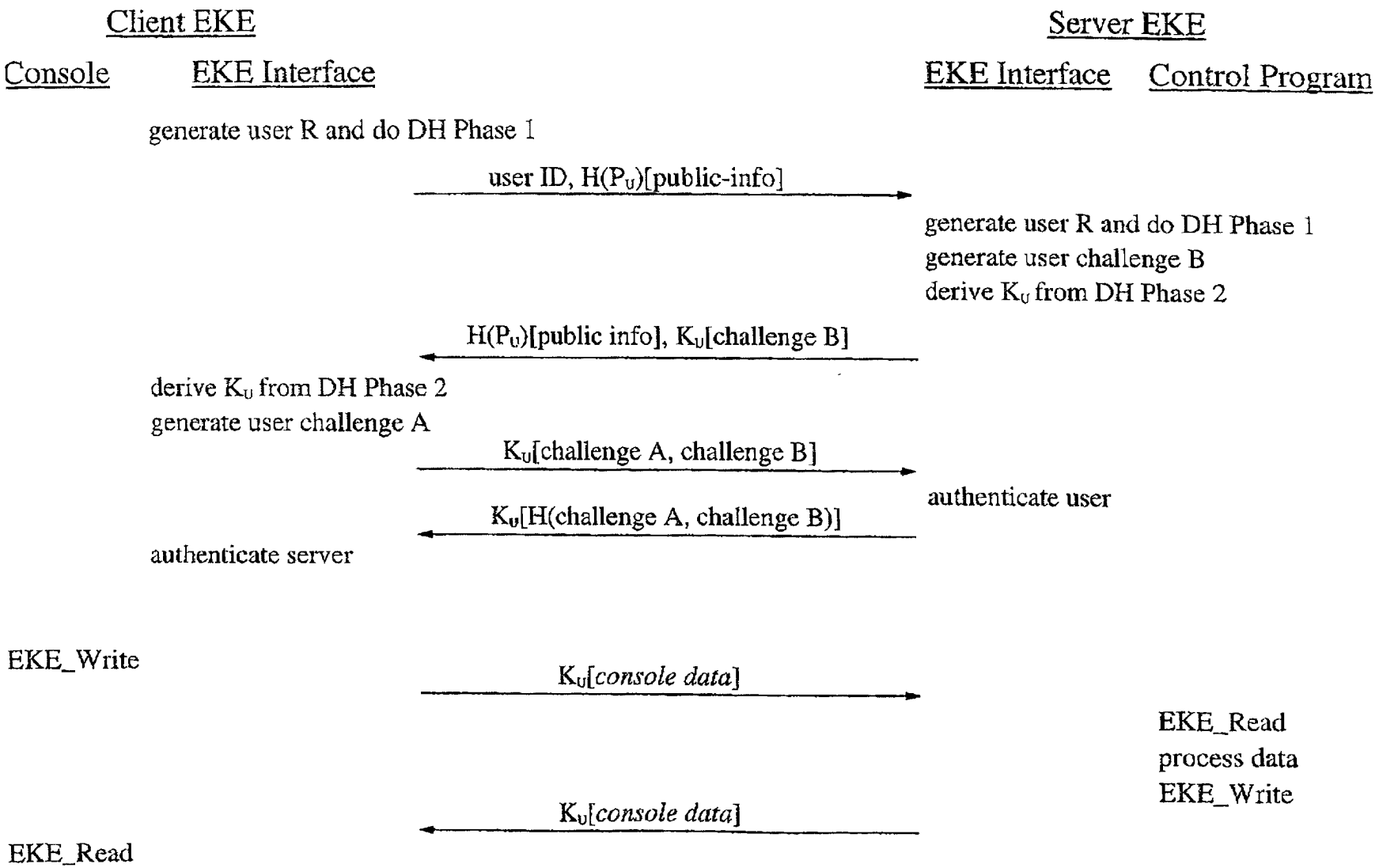

Client EKE
Server EKE
Console
EKE Interface
EKE Interface
Control Program
generate user R and do DH Phase 1
user ID, H(P_U)[public-info]
generate user R and do DH Phase 1
generate user challenge B
derive K_U from DH Phase 2
H(P_U)[public info], K_U[challenge B]
derive K_U from DH Phase 2
generate user challenge A
K_U[challenge A, challenge B]
authenticate user
K_U[H(challenge A, challenge B)]
authenticate server
EKE_Write
K_U[console data]
EKE_Read
process data
EKE_Write
K_U[console data]
EKE_Read

FIG 4A

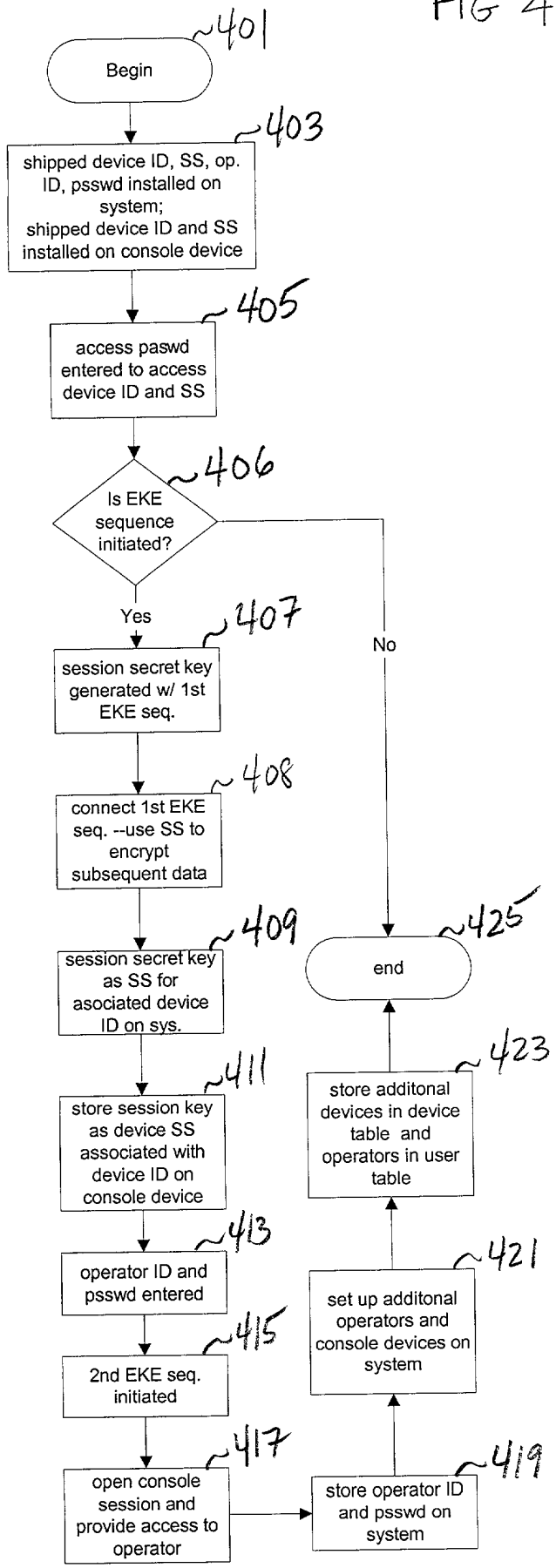

401
Begin
403
shipped device ID, SS, op. ID, psswd installed on system;
shipped device ID and SS installed on console device
405
access paswd entered to access device ID and SS
406
Is EKE sequence initiated?
Yes
No
407
session secret key generated w/ 1st EKE seq.
408
connect 1st EKE seq. --use SS to encrypt subsequent data
409
session secret key as SS for asociated device ID on sys.
411
store session key as device SS associated with device ID on console device
413
operator ID and psswd entered
415
2nd EKE seq. initiated
417
open console session and provide access to operator
419
store operator ID and psswd on system
421
set up additonal operators and console devices on system
423
store additonal devices in device table and operators in user table
425
end

FIG. 4B

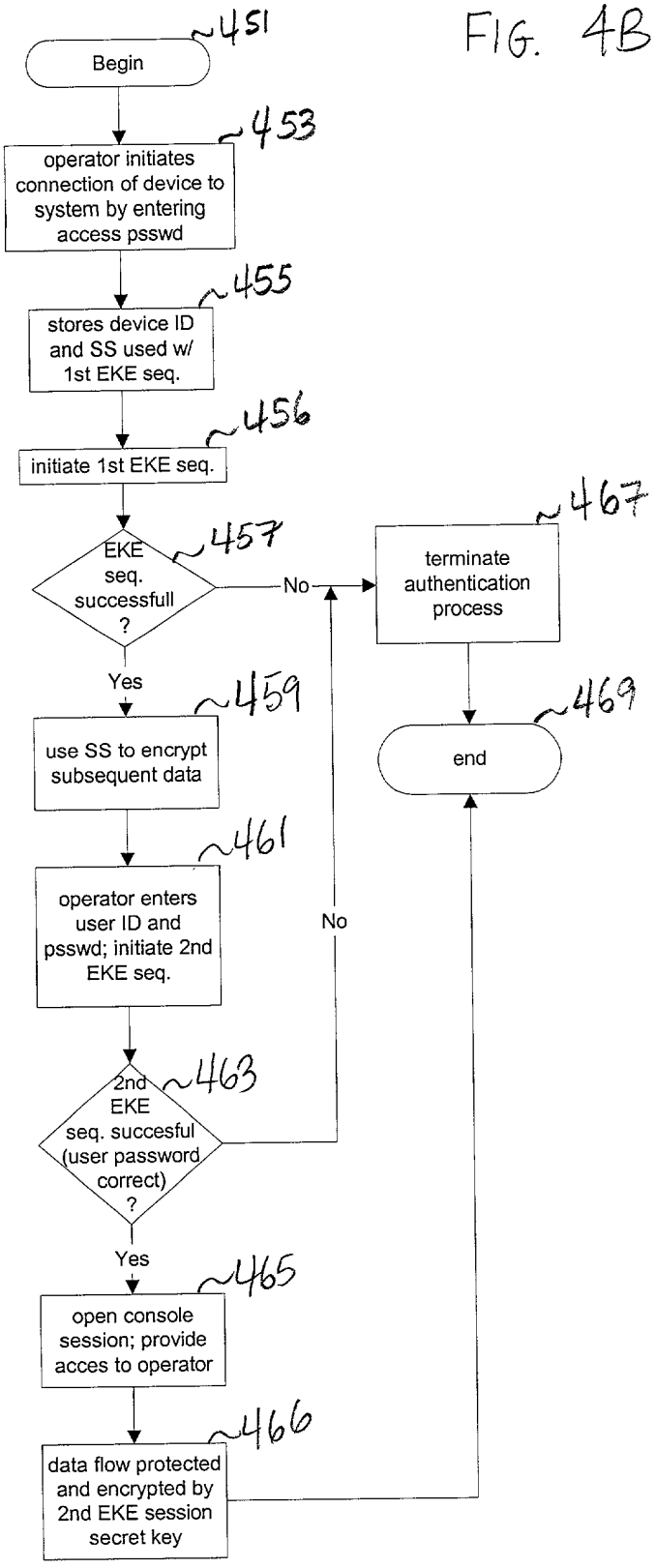

Begin
451
operator initiates connection of device to system by entering access psswd
453
stores device ID and SS used w/ 1st EKE seq.
455
initiate 1st EKE seq.
456
EKE seq. successfull ?
457
No
terminate authentication process
467
Yes
use SS to encrypt subsequent data
459
end
469
operator enters user ID and psswd; initiate 2nd EKE seq.
461
No
2nd EKE seq. succesful (user password correct) ?
463
Yes
open console session; provide acces to operator
465
data flow protected and encrypted by 2nd EKE session secret key
466

FIG 5A

Client Device (PC) 501

Server Connection	
Server1	Hash (device identifier, shared secret)
Server2	Hash (device identifier, shared secret)

FIG 5B

Server

Device Table 511

Device Identifier	Hashed shared secret
QCONSOLE	H(shared secret)
DEVICE2	H(shared secret)

User Table 513

User Identifier	Hashed password
11111111	H(password)
22222222	H(password)
QSRV	H(password)
QSECOFR	H(password)